Steganography in MAC Layers of 802.15.4 Protocol for securing Wireless Sensor Networks

David Martins, Hervé Guyennet

Steganography in MAC Layers of 802.15.4 Protocol for securing Wireless Sensor Networks

David Martins and Hervé Guyennet
Computer Science Department
University of Franche-Comté, France
Email: {dmartins,hguyennet}@lifc.univ-fcomte.fr

***Abstract*—In many applications, wireless sensor networks need to secure information. Actual researchs found efficient solutions for this kind of network, principally by using cryptography to secure the data transfer. However an encrypted information send by the network can be sufficient to prevent an attacker, who eavesdrops the network, that something important has been detected. To avoid this situation, we propose another way to secure wireless sensor networks by using steganography, specifically by hiding data in the MAC layer of the 802.15.4 protocol. We show that this solution can be an energy-efficient way with a good latency to hide data in a wireless sensor network.**

***Index Terms*—wireless sensor networks, steganography, security, 802.15.4 protocol, MAC layer, hidden data**

I. Introduction

Steganography is an old technique that has existed since antiquity. Herodotus, a Greek historian who lived in the 5th century B.C., relates how the Greeks sent and received warnings of enemy movements using a message underneath the wax of a writing tablet. Other examples were the use of secret ink to hide information on a white paper or the use of micro-dot by intelligence agencies in World War 2.
The word steganography comes etymologically from the Greek words *Stegano*, meaning *I cover*, and *Graphô*, meaning *I write*, and is literally *cover what I write* - or more simply, hide data. If cryptography is to encrypt and render a data unreadable, steganography is the way to hide the existence of this data.

In this paper, we show that it is possible to secure a wireless sensor network, to use steganographic techniques to hide the existence of data in the 802.15.4 protocol. This protocol is a protocol widely used in wireless sensor networks. This protocol specifies the PHY and MAC layers of communication, because it provides an energy-efficient solution for communication between wireless sensors. Zigbee [1], the most used protocol in wireless sensor networks, uses this 802.15.4 protocol for the communication layer. We explain in this article how we can use the MAC layer fields of 802.15.4 protocol to hide data in the network and create a steganographic channel. By using steganographic methods, this data becomes undetectable in the wireless sensor network if this steganographic method is unknown by an attacker.
In Section 2 of this paper, we present previous work on steganography and specifically in communication protocols. In Section 3, we show different possibilities of hiding data in wireless sensor networks by using MAC layer fields of the 802.15.4 protocol. In Section 4, we describe an experiment of steganography in wireless sensor networks that we made with telosB sensors. In Section 5, we show our experimental results of simulations with AvroraZ by comparing energy consumption and latency of steganography in MAC layer of 802.15.4 protocol and cryptography. In Section 6, we discuss about our future works and we conclude.

II. Related work

The aim of steganography consists of embedding data (text, movie, picture, etc...) called the secret message, in another media or support [2]. The support where the data is hidden is named the cover object. Once the secret message is embedded in the cover message, the result is called a stego object. For example, we can hide a picture in another picture, and in this latter picture, we cannot see that the first picture is hidden inside.
When we speak about steganography, we refer to the analogy of Alice and Bob [3]. Alice and Bob are in jail and are monitored by a warden, Wendy. If Alice wants to send a message to Bob, this message must go through Wendy. If Wendy sees that the message contains an important message (for example the hour of an escape), Wendy will never give the message

to Bob. Therefore, Alice should find a way to hide information in the message without Wendy seeing it. For example, Alice will hide a message in another message. If we read every other letter, we can read the hidden message; but if Wendy reads this message, she will not see the hidden message. In steganography, this example shows that the steganographic method must be kept secret (if Wendy knows the steganographic technique, she can read the message) and all participants who want to communicate should know this method to hide and to read the data.

A lot of steganographic techniques exist [3], but the most important goal of actual research work in steganography is to hide pictures in an other picture. These techniques have given birth to watermarking [4], which consists of watermarking a picture to add data. For example, watermarking can be used to add the name of a patient or private information to a medical picture (scanner, radiography, MRI).

Several steganographic techniques aim to use specificities of communication protocols to hide data and use communication layer fields as the cover object. This use of steganographic data in communication layer fields provides the creation of a hidden channel in the network. Only devices that know in which fields the data is hidden can read data or write data. They can invisibly exchange data in the network if the network does not know the steganographic technique.

[5], [6] and [7] show different possibilities for hiding data by using specificities of protocol to create a hidden channel (steganographic channel). The most used techniques consist of using the reserved field of the protocol. Thus, [5] uses the reserved field in the TCP packet header of the TCP/IP protocol, as we can see in Figure 1, and gives the possibility to hide six bits per exchanged packet in this example.

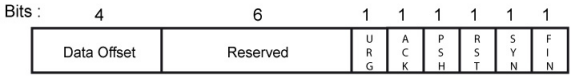

Fig. 1. Reserved bytes in TCP Packet Header

This technique can also be used to create a hidden channel in a wireless local area network as explained in [8]. This example is closer to what we can do in wireless sensor networks if we try to apply this method in the 802.15.4 protocol.

In wireless sensor networks, the use of steganography has been first mentioned in [9], with the conclusion that it would be difficult to apply it in wireless sensor networks, because they are constrained by their limited energy and their low-power computing, and because steganography is more applied with picture or video. However [10] and [11] show possibilities using noise in the physical layer of the 802.15.4 protocol to hide data and create a steganographic channel. If these examples are known possibilities for using the 802.15.4 protocol to hide data, and show that steganography is a new way of research in wireless sensor network, to the best of our knowledge [12], we do not know of an example of steganography using communication of MAC layer fields in the 802.15.4 protocol.

III. Hiding data in MAC IEEE 802.15.4

In this section, we show the possibility of hiding data in the MAC layer of the 802.15.4 protocol.

Frames in the MAC layer of the 802.15.4 protocol are different and depend on the kind of packet sent. The MAC layer uses 4 different kinds of frames:

1) - *Data frame*
2) - *Beacon frame*
3) - *Acknowledgment frame*
4) - *MAC command frame*

We will discuss ways to hide data in these different kinds of frames.

A. Data frame

The general structure of a MAC data frame can be seen in Figure 2. This structure can be found in [13].

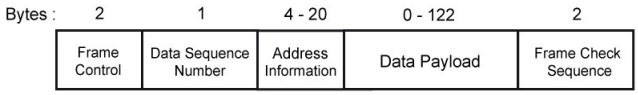

Fig. 2. MAC data frame structure

In this frame, the Frame Control field, Data Sequence Number field, and Address Information field provide possibilities to hide information.

1) Frame control field: The Frame Control field is represented by Figure 3.

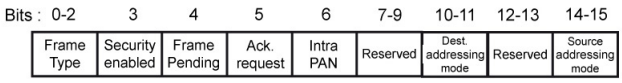

Fig. 3. Frame control field structure

We can see that the 7-9th bits and the 12-13th bits are reserved and can be used to hide a stego object. Here, we can encode three and two bits, respectively, in these fields.

2) Sequence Number field: The Sequence Number field contains the numbering of each packet on 8 bits, used in particular with packet acknowledgements to specify which packet has been acknowledged. The value of this number corresponds to the PIB macDSN variable. This variable is initialized randomly, then incremented after each received packet.
If we choose this initialized number of the PIB variable, we can hide a stego object (or a part of the stego object) inside. We can hide up to one byte of data in this field.

3) Address Info field: The Address Info field is represented in Figure 4. Its size varies between four and 20 bytes.

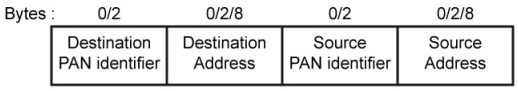

Fig. 4. Address Info field structure

The Source Address field is interesting, because we can choose to have a short (16 bits) or an extended source address (64 bits). It is possible to hide data in this field, for example, if we specify a nonexistent source address. With this nonexistent address, we can hide a stego object with a size up to 64 bits. This steganographic technique can be particularly undetectable if the network does not know the exact number of nodes present in the network, especially in a big network where nodes can be added over time.

B. Beacon frame

The general structure of a MAC Beacon frame can be seen in Figure 5.

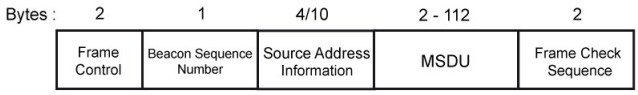

Fig. 5. Beacon frame structure

We find the same possibilities for hiding information as in the Data Frame, in the Frame Control and in the Source Address Information field. However, in the Beacon Frame, the source address information is limited to 10 bytes; yet the Beacon Sequence Number field give us another way to use the cover object.
The Beacon Sequence Number field contains the sequence number of the Beacon node. This number is given by the macBSN variable. This variable is ordinarily initialized randomly. As in the Sequence Number field of the MAC data frame, we can voluntarily choose the value of this number and then hide up to one byte of data.

C. Acknowledgement frame

The general structure of an Acknowledgement frame can be seen in figure 6.

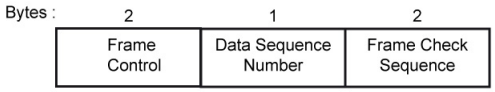

Fig. 6. Acknowledgement frame structure

We find the same possibilities for hiding data in the Frame Control field and Data Sequence Number field. Both are identical to fields of the MAC data frame.

D. Command frame

The general structure of a command frame can be seen in figure 7.

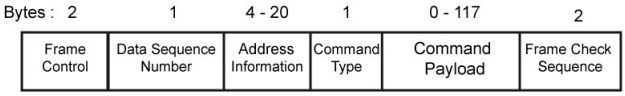

Fig. 7. Command frame structure

Here, we can see that the Frame Control, Data Sequence Number and Address Information fields provide the same possibilities of hiding data in the command frame as in the MAC data frame.

IV. Experimentation

A. Our proposition

The aim of our proposition to use steganographic methods is to propose a energy-efficient solution to hide information and answer to the example of Alice, Bob and Wendy applied in wireless sensor networks: where Alice and Bob would be two sensors, and Wendy would be another sensor or a device of an attacker that listens to network communications. If Wendy sees that an encrypted message is sent by Alice to Bob, she can think that an important information is hidden in this message. In the case of a network that detects intrusions or a wireless sensor network that sends data about troop's positions for a military application, to see an encrypted message can be sufficient to know if the network has detected something or to know where troops move. To counter this problem, we propose that sensors of the network, that detect important information, send unimportant information in the data

payload (for example a routing data), and send the critical data in MAC layer fields of the 802.15.4. As we saw in the previous section, the MAC layer provide us a lot of possibilities for cover objects. there are other possibilities for hiding data in the 802.15.4, but we have chosen to present the most significant parts.
If we take the example of a sent MAC data frame, we can hide in the different fields that we have seen previously :

1) *3 + 2 = 5 bits for the frame control field*
2) *8 bits for the data sequence number field*
3) *64 bits for the address info field*

...making a total of 77 hidden bits. This number of bits is enough to exchange one or more stego messages, as a GPS position, a temperature or just a code.
In our threat model, we assume that the attacker does not know these steganographic possibilities and that for the attacker an encrypted data is more important than an unencrypted data.

B. Implementation

To prove the feasibility of using steganography in MAC layer fields of 802.15.4 protocol, we implement a program on telosB sensors in TinyOS 2.x using the tkn154 library [14], that provides to modify MAC layer fields of 802.15.4 protocol. For our experiment we use 3 telosB sensors:

- a sender, that detects information and sends it with steganography
- an intermediate that makes the relay between the sender and the receiver
- a receiver connected to a computer that displays steganographic data recorded in MAC Layer.

The program of the sender sensor records temperature data that it sends to the intermediate all seconds in a different steganographic field (macDSN field or Source Address field) of the MAC layer of a Data Frame. Our results show that for 100 records, all data have been transmitted using steganography from the sender to the receiver without any loss.

V. Experimental Results

We use AvroraZ [15] for our simulation. Avroraz is a specific version of the Avrora simulator [16] for wireless sensor network, that includes simulation of MAC layer of 802.15.4 for micaZ sensors. This simulator give us the opportunity to record execution time and energy consumption of our proposition. Following tables and figures show results of the simulation, where we hide data in the MAC layer fields of MAC Data Frame of 802.15.4 protocol. We call here StegoMacDSN, StegoShortAddress, StegoExtendedAddress and StegoAllFields, respectively the fact to hide data in the macDSN field, the Short Address Source field, the Extended Address Source field and the combination of the macDSN, the Extended Address Source and reserved bits fields. We compare our steganographic solutions with the symetric encryption algorithm AES 128 used in wireless sensor network, principaly with the secure protocol TinySEC [19]. Results are showed in the table 1.

Method (Bits hidden/encrypted)	Number of CPU Cycle	Execution time (μsec)	Energy Consumption (μJoule)
StegoMacDSN (8)	60	8.14	0.1031
StegoShortAddress (16)	108	14.65	0.1855
StegoExtendedAddress (64)	112	15.19	0.1924
StegoAllField (77)	178	24.14	0.2955
AES 128 (1 to 128)	3843125	521257.19	6604.4328

TABLE I
Number of CPU cycles, execution time and energy consumption results on micaZ

Obviously we can see that executions of our steganographic solutions are extremly quicker than cryptography and energy-efficient.

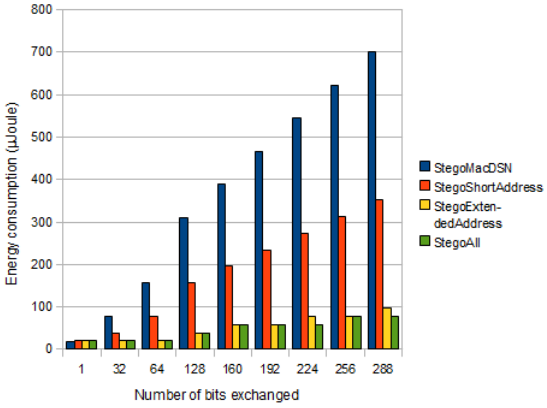

Fig. 8. Energy consumption to hide and send a stego message on micaZ

The figure 8 shows the energy consumption to hide and send a stego message, depending on the data size of this message. We can see that even the worst solution StegoMacDSN, which consists to only use the macDSN layer and to send a packet for each 8 bits, costs less energy to do than encrypt this message with AES 128.

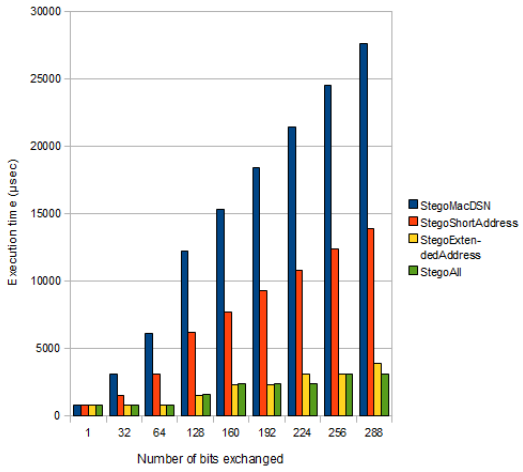

Fig. 9. Time execution to hide and send a stego message on micaZ

The figure 9 shows the execution time necessary to hide and send a stego message, depending on the data size of the message. Results show that the solution of steganography in wireless sensor network can be adapted for reactive application, even if the size of cover objects are shorts.
In conclusion, results of simulation proove that steganography in the Mac layer of 802.15.4 protocol give us new energy-efficient possibilities to hide data with a good latency in wireless sensor networks.

VI. Future Work and Conclusion

Our proposition to hide information in MAC Layer of 802.15.4 protocol, is a pure steganographic solution. It means that the secret is where the data is hidden, but obviously if an attacker know this secret, he is able to read the message. This is why, after showing that steganography is possible in 802.15.4 protocol, we want next to implement secret key and public key steganography to enforce the security. Our final aim is to implement a steganographic method in the 802.15.4 protocol that resists to steganalysis.

However we show in this paper that it is possible to use steganography to hide information in the MAC layer of the 802.15.4 protocol. We have implemented this solution on TelosB sensor and simulate their energy-consumption and their latency with Avroraz. Our final results show that steganography in 802.15.4 protocol provides an energy-efficient solution with a low latency to secure and to hide data in wireless sensor networks.

References

[1] Z. Alliance, "In http://www.zigbee.org."

[2] R. Anderson and F. Petitcolas, "On the limits of steganography," *IEEE Journal of Selected Areas in Communications*, vol. 16, pp. 474–481, 1998.

[3] S. Katzenbeisser and F. A. Petitcolas, eds., *Information Hiding Techniques for Steganography and Digital Watermarking*. Norwood, MA, USA: Artech House, Inc., 2000.

[4] I. Cox, M. L. Miller, and J. A. Bloom, *Digital watermarking*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2002.

[5] T. G. Handel and M. T. Sandford, II, "Hiding data in the osi network model," in *Proceedings of the First International Workshop on Information Hiding*, (London, UK), pp. 23–38, Springer-Verlag, 1996.

[6] Z. Trabelsi, H. El Sayed, L. Frikha, and T. Rabie, "A novel covert channel based on the ip header record route option," *Int. J. Adv. Media Commun.*, vol. 1, no. 4, pp. 328–350, 2007.

[7] S. J. Murdoch and S. Lewis, "Embedding covert channels into tcp/ip," in *Information Hiding: 7th International Workshop, volume 3727 of LNCS*, pp. 247–261, 2005.

[8] K. Szczypiorski, "A performance analysis of hiccups - a steganographic system for wlan," *CoRR*, vol. abs/0906.4217, 2009.

[9] A.-S. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in wireless sensor networks: Issues and challenges," *CoRR*, vol. abs/0712.4169, 2007.

[10] L. S. Mehta A.M. and P. K., "Steganography in 802.15.4 wireless communication," in *Advanced Networks and Telecommunication Systems, 2008. ANTS '08. 2nd International Symposium on*, (Mumbai), pp. 1–3, 2008.

[11] T. Kho, "Steganography in the 802.15.4 physical layer," tech. rep., 2007.

[12] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 1-4, pp. 6–28, 2008.

[13] "Ieee 802.15.4. 2003. part 15.4: Wireless medium access control and physical layer specifications for low rate wireless personal area networks.," tech. rep., ANSI/IEEE Standard 802.15.4, Sept.

[14] J. hinrich Hauer, D. ing Adam, and W. Abstract, "Tkn technical reports series," 2009.

[15] R. de Paz Alberola and D. Pesch, "Avroraz: extending avrora with an ieee 802.15.4 compliant radio chip model," in *PM2HW2N '08: Proceedings of the 3nd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, (New York, NY, USA), pp. 43–50, ACM, 2008.

[16] B. L. Titzer, D. K. Lee, and J. Palsberg, "Avrora: scalable sensor network simulation with precise timing," in *IPSN '05: Proceedings of the 4th international symposium on Information processing in sensor networks*, (Piscataway, NJ, USA), p. 67, IEEE Press, 2005.

[17] L. J. Roman R., Jianying Zhou, "Applying intrusion detection systems to wireless sensor networks," in *Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE*, pp. 640–644, January 2006.

[18] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, pp. 393–422, 2002.

[19] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: a link layer security architecture for wireless sensor networks.," in *SenSys* (J. A. Stankovic, A. Arora, and R. Govindan, eds.), pp. 162–175, ACM, 2004.